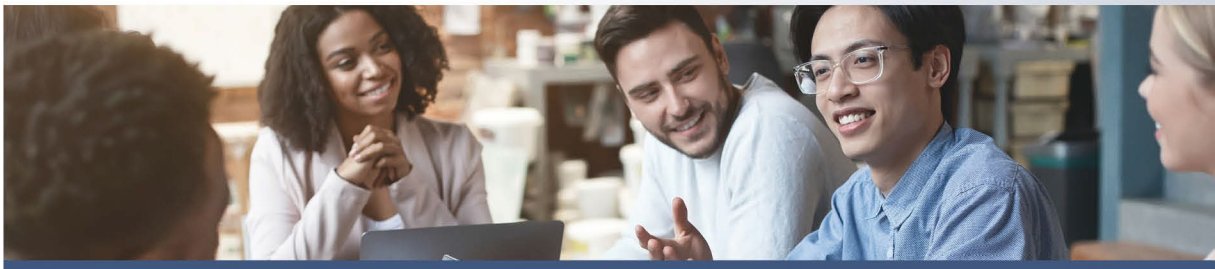
Provided by Risk Strategy Solution

RISK ADVISOR

April 2024



COMMERCIAL

Benefits and Risks of Rooftop Solar Panels for Commercial Properties

Although solar panels can provide significant financial, environmental and reputational benefits, they can present various risks and be susceptible to damage from several sources. Therefore, as the popularity of solar panels increases, commerical property owners need to be aware of their benefits and disadvantages to make the best decision for their buildings.

Solar Panels' Benefits for Commercial Properties

Installing solar panels on commercial rooftops offers several benefits for commercial properties, including:

- Cost savings on electric bills
- Tax incentives
- Reduced carbon emissions
- Improved reputation by demonstrating a commitment to sustainability
- Alternative solution during power grid outages
- Increased property value

The Risks of Rooftop Solar Panels

Although solar panels offer several benefits, there are risks for businesses to consider:

- Fire hazards and the risk of fires that produce toxins
- Susceptibility to weather- and animal-related damage
- Added weight that can have structural implications
- Decreased rooftop walking space, creating fall risks
- Attractive target for theft and vandalism

Mitigating the Risks of Rooftop Solar Panels

As property owners weigh the pros and cons of rooftop solar panels, they should also consider the following measures to mitigate risks associated with them:

- **Choose quality materials** while considering their combustibility and toxicity.
- **Have a professional evaluate the rooftop** to ensure it can handle the weight of solar panels.
- **Examine insulation materials** to determine if they present additional fire risks.
- **Hire certified installers** to help make certain the systems are installed following the manufacturer's instructions and any applicable codes or regulations.
- **Ensure the solar panels' inverter is properly placed** in a structurally sound, dry area away from combustible materials.
- **Have certified technicians conduct regular inspections and maintenance** to help identify and remediate issues before they evolve into larger problems.
- **Take protective measures**, including removing overhanging trees; installing animal guards, an arc fault detection device and security systems, ensuring enough space is available to walk around them and informing technicians about their presence; and selecting solar panels rated to withstand the severe weather or seismic risks common to the area.
- **Utilize fire alarms and suppression systems** that can provide alerts for fires and extinguish or slow them if they emerge. There should also be sufficient roof access for firefighters, a fire risk assessment should be conducted, and an emergency action plan should be in place to swiftly respond to fires and toxic fumes.

Additionally, businesses should work with a licensed insurance professional to review their insurance coverage and ensure their policies cover solar panels and their associated risks.

Contact us today for more risk management information.

Risk Strategy Solutions

5 Common Cybersecurity Myths Debunked

Cybersecurity consists of strategies implemented to help protect organizations from cyberattacks and related losses. Such defense has become increasingly important as businesses of all sizes and sectors expand their reliance on technology and other digital services. Yet, there are several misconceptions about cybersecurity that diminish the value of effective mitigation strategies and may leave organizations vulnerable to cyberthreats. Here are five common cybersecurity myths, debunked:

Myth #1: Only large corporations need cybersecurity protocols.

A common misconception is that adopting proper cybersecurity measures only makes sense for large corporations. While large organizations can be susceptible to cyberattacks, this doesn't mean small businesses are immune to them. On the contrary, some cybercriminals consider small organizations more attractive targets because they are more likely to have weaker cybersecurity measures, which simplifies the overall attack process.

Myth #2: Basic cybersecurity procedures are sufficient to protect against possible threats.

For certain organizations, cybersecurity consists of a few basic protocols, such as deploying firewalls and installing antivirus software. These can prove useful, but adopting a single-layered approach probably isn't effective in minimizing all threats, including brute force incidents and social engineering scams. As the cyber risk landscape changes, organizations' mitigation strategies should follow suit. Leveraging a wide range of multilayered protective measures (e.g., multifactor authentication, endpoint detection and response solutions, email authentication technology, patch management plans and data backup systems) can better equip organizations to address their digital exposures.

Myth #3: Cybersecurity measures aren't worth the cost for small businesses.

Small organizations may initially be less inclined to invest in cybersecurity due to the expenses. This likely stems from these organizations thinking that cybersecurity benefits aren't worth their costs. However, small businesses are frequent targets for cyberattacks, and these businesses are more likely to face financial ruin in the aftermath of such attacks. Considering this, investing in sufficient mitigation strategies could make all the difference in helping these small businesses avoid major losses and prevent financial devastation from cyber incidents.

Myth #4: Cybersecurity is only the IT department's job.

Although IT professionals play a major role in implementing adequate cybersecurity measures, the most effective cybersecurity models involve companywide participation. Without this, organizations are more likely to have poor cyber hygiene and awareness. As such, it's imperative that organizations foster a culture that encourages everyone to take responsibility for cybersecurity. This entails having company executives lead by example, training employees to detect and defend against prevalent cyberthreats, and recognizing those who demonstrate a continued commitment to security.

Myth #5: Cyberthreats are always external.

In addition to external sources, cyberthreats can arise from insiders, including employees, vendors or third-party collaborators. Due to their unique privileges, insider threats can potentially compromise organizations' most valuable assets and leave the business more susceptible to a range of cyber incidents. In fact, a recent survey conducted by IT platform Cybersecurity Insiders found that the average insider event costs over $755,000. Therefore, it's vital for organizations to account for both external and internal threats when developing their cybersecurity measures.

Accurate information is essential to an effective cybersecurity program. For more risk management guidance, contact us today.

A recent study by Accenture, an international IT services and consulting company, found that **43% of all cyberattacks target small businesses**. With this in mind, it's clear that cybersecurity measures are necessary for organizations of all sizes.